Annual 47 C.F.R. § 64.2009(e) CPNI Certification Template

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2019 covering the prior calendar year 2018

1. Date filed: February 12, 2019
2. Name of company(s) covered by this certification: Faith Municipal Telephone Company
3. Form 499 Filer ID: 808185
4. Name of signatory: Debbie Brown
5. Title of signatory: Finance Officer
6. Certification:

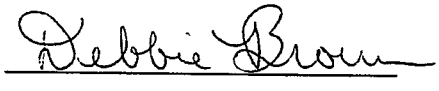
I, Debbie Brown, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, safeguards, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken actions (*i.e.*, proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47. C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed 

Attachments: Accompanying Statement explaining CPNI procedures

City of Faith Telephone Company (ID: 808185)

OPERATING PROCEDURES FOR COMPLIANCE WITH CPNI RULES

Faith Municipal Telephone Company (the "Company") has implemented the following procedures to ensure that it is compliant with Part 64 of Title 47 of the Code of Federal Regulations, Subpart U – Customer Proprietary Network Information (CPNI), § 64.2001 through § 64.2011.

Compliance Officer

The Company has appointed Debbie Brown to act as the CPNI Compliance Officer. The Compliance Officer is responsible for ensuring that the Company is in compliance with all of the CPNI rules. The Compliance Officer is also the point of contact for anyone (internally or externally) with questions about CPNI.

Employee Training

The Compliance Officer arranges for the training of all employees on a regular basis, and more frequently as needed. Any new employee is trained when hired by the Company. The training includes, but is not limited to, when employees are and are not authorized to use CPNI, and the authentication methods the company is using.

After the training, all employees are required to sign a certification that they have received training on the CPNI rules, that they understand the Company's procedures for protecting CPNI and they understand the Company's disciplinary process for improper use of CPNI.

Employees are instructed that if they ever have any questions regarding the use of CPNI, if they are aware of CPNI being used improperly by anyone, or if they encounter someone other than the authorized person on an account trying to access CPNI that they should contact the Compliance Officer immediately. The Compliance Officer will then determine what actions needs to be taken.

Disciplinary Process

The Company has established a specific disciplinary process for improper use of CPNI. The disciplinary action is based on the type and severity of the violation and could include any or a combination of the following: retraining the employee on CPNI rules, notation in the employee's personnel file, formal written reprimand, suspension or termination.

The disciplinary process is reviewed with all employees.

Customer Notification and Request for Approval to Use CPNI

The Company has not provided notification to its customers and has not asked for approval to use CPNI because it only uses CPNI in those instances where it is permissible to use CPNI without customer approval. It does not share the customer's CPNI with any joint venture partner, independent contractor or any other third party.

If the Company receives a call from a customer who wants to discuss services outside of the customer's existing service offerings, the customer service representative uses the oral notification for one-time use of CPNI to obtain approval for the duration of the call only.

If, in the future, the Company decides to ask customers for approval to use their CPNI, it will implement a system by which the status of a customer's CPNI approval can be clearly established prior to the use of CPNI.

Marketing Campaigns

The Company does not conduct any marketing campaigns. If, in the future, the Company decides to have a marketing campaign, it will establish a supervisory review process and a process for maintaining a record of the campaign before any campaign is conducted.

Authentication

The Company does not disclose any CPNI until the customer has been appropriately authenticated as follows:

In-office visit - the customer must provide a valid photo ID matching the customer's account information.

Customer-initiated call – the customer is authenticated by providing an answer to a pre-established question and must be listed as a contact on the account.

If the customer wants to discuss call detail information that requires a password, the following guidelines are followed:

- If the customer can provide all of the call detail information (telephone number called, date of the call, the amount of the call, etc.) necessary to address the customer's issue, the Company will continue with its routine customer care procedures.

- If the customer cannot provide all of the call detail information to address the customer's issue, the Company will: (1) call the customer back at the telephone number of record, (2) send the information to the address of record, or (3) ask the customer to come into the office and provide a valid photo ID.

Notification of Account Changes

The Company promptly notifies customers whenever a change is made to the following:

- Address of record.

The notification to the customer will be made either by a Company-originated voicemail or sent to the address that has been associated with the account for at least 30 days. It will not be sent to the new address.

The Company's billing software generates a letter to the customer whenever a change is made to the address.

Notification of Breaches

Employees will immediately notify the Compliance Officer of any indication of a breach. If it is determined that a breach has occurred, the Compliance Officer will do the following:

- Notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) as soon as practicable, but in no event later than 7 business days after determination of the breach. The notification will be via the FCC link at http://www.fcc.gov/eb/cpni.

- Notify customers only after 7 full business days have passed since notification to the USSS and the FBI, unless the USSS or FBI has requested an extension.

- If there is an urgent need to notify affected customers or the public sooner to avoid immediate and irreparable harm, it will be done only after consultation with the relevant investigating agency.

- Maintain a record of the breach, the notifications made to the USSS and FBI, and the notifications made to customers. The record will include dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.

- Include a summary of the breach in the annual compliance certificate filed with the FCC.

Annual Certification

The Compliance Officer will file a Compliance Certification with the FCC by March 1 of each year for data pertaining to the previous calendar year.

Record Retention

The Company retains all information regarding CPNI. Following is the minimum retention period the company has established:

- Breaches – two years
- Annual certification – seven years
- Employee training certification – two years
- All other information – two years